Monthly Security Tips Newsletter
December 2007

CISO Tips

Protect your home computer from access to unsafe and undesirable sites.
Try Blue Coat's™ free home offering at http://www1.k9webprotection.com/;

Remember, reputable financial institutions NEVER ask for personal information [via email or the Internet] such as social security numbers, account numbers or PINs. Always be sure that websites are secured (see below and last month's tips on PHISING) before revealing personal information.

To view State security policies, please visit: http://isd.alabama.gov/policies/policies.aspx?sm=c_a;

Online Shopping

The volume of individuals doing their shopping online continues to increase, especially during the holiday season. While online shopping may provide benefits for consumers, there are also risks that you must understand.

Below are some tips to follow for a safe online shopping experience.

Update your software. Before you shop online, ensure you have the most current security software updates available for your operating system, applications and browser. Set your default settings to "auto update."

Know with whom you are doing business. You are safest when doing business with a reputable company. If you are not familiar with the company, use a search engine to investigate customer reviews of the seller. Consider website rating software or toolbars, or consider using web site rating services or product locator services on the Internet. Be wary of unrealistic low prices that seem too good to be true. They may be an attempt to trick you into clicking on a malicious link.

Ensure "pay online" transactions are secure.

- Be sure "https" or "shttp" appears in the web site's address bar when you are ready to provide payment information.
- Look for logos from organizations that feature trusted or credential websites like **BBBOnline**, **TRUSTe** or **Verisign**.
- Use credit cards to pay for online purchases because they usually offer theft, fraud, and vendor non-performance protection. Debit cards have less protection as the money is deducted immediately from your account and you must pursue refunds or recovery of funds individually.
- Do not send financial payment or credit card information through email.
- Do not provide bank account or Social Security numbers to complete an online transaction. Be wary of anyone who requests this type of information online.
- Do not perform online transactions from a public computer or kiosk.
- Do not use your browser to store password or credit card information.

- Do not enter personal information in a pop-up screen. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens.

Understand the website's "privacy policy." Read the website's privacy policy: how will the company use your personal information? Be suspicious if a website's privacy policy is nonexistent. Research and understand what the seller does with your private information. If you can't find this information, shop at another website.

Use strong passwords. When creating passwords for online accounts, use at least eight characters, with numbers, special characters and upper and lower case letters whenever possible. Don't use the same password for online shopping websites that you use for non-shopping web sites or for computer programs on your local computer. Never use obvious passwords or share logins and passwords.

Check your credit card and bank statements regularly. Check or reconcile your credit card and bank statements regularly. Immediately report any anomalies or transactions you didn't make to your credit card company or bank.

Use temporary account authorizations when available. Some credit card companies may offer virtual or temporary credit card authorization numbers. This kind of service gives you use of a secure and unique account number for each online transaction. These numbers are often issued for a short period of time and cannot be used after that period. Contact your credit card company to see if they offer this service.

Share your online shopping knowledge with family and friends. Take the knowledge you gain from this Cyber Security Tip and talk about it with others. The more you share these tips, the safer and more secure we all can be.

General Shopping Tips

Understand the "terms" of the transaction. When shopping online, understand the terms of the transaction, including incentives, shipping and/or handling costs, return or exchange policies and timelines, restocking or return costs, product quality claims, minimum purchase limits, etc.

Keep a good paper trail. Keep copies of all transactions including the product description, price, the online receipt, any emails you exchanged leading up to and including the transaction.

For more online shopping information visit:

Federal Trade Commission: www.ftc.gov/onlineshopping/
OnGuard Online: www.onguardonline.gov/shopping.html
Stay Safe Online: www.staysafeonline.info/basics/shoppingTips.html
Safeshopping.org: www.safeshopping.org/tips.shtml

For more monthly tips visit: www.msisac.org/awareness/news/

MS-ISAC

http://www.msisac.org